Electronic Version

Stylesheet Version v1.1.1

Description

[Method to enable a Homeland Security "heartbeat"]

Cross Reference to Related Applications

[0001] See Utility Patent Filing, application number 10/605144, EFS ID 47552, date time group (DTG) 2003-09-11 10:55:59 EDT entitled "method to commercialize structured military messaging"by Steven McGee

Federal Research Statement

[0002] [See Utility Patent Filing, application number 10/605144, EFS ID 47552, date time group (DTG) 2003-09-11 10:55:59 EDT entitled "method to commercialize structured military messaging" by Steven McGee]

Background of Invention

[0003] This utility patent application describes a method to leverage an existing part commercial part military unique "heartbeat"mechanism as seen on various television documentaries and news channels as implemented by the

United State Army"s Force XXI Battle Command Brigade and Below (FBCB2) application. FBCB2 distributes friendly force unit location data and potential hostile forces on an adhoc basis (e.g., SPOT reports) over tactical radio nets. The core mechanism that FBCB2 leverages is referred to the heartbeat[1] that consists in part TCP/IP"s (Transport Control Protocol/Internet Protocol) intrinsic timers, events and message functions that are commercial, ubiquitous and universal as TCP/IP itself. What makes FBCB2"s heartbeat implementation Government Off the Shelf (GOTS) is the fact that FBCB2 sends collected data using a proprietary military message protocol/format (Variable Message Format VMF) via government developed message parsers that generate the VMF messages that are compressed binary and bandwidth friendly. See previous patent application cited by this applicant for the shortfalls of VMF and other GOTS produced messaging mechanisms/formats. The gist of this claim is that the main difference between military networks and commercial is the proprietary message formats on the military side of the house that are slowly being converted to XML schemas is a segue to improve homeland security by making the whole process commercial and open by using commercial tools and

frameworks.

SUMMARY OF INVENTION

[0004] Principle operation of the invention: commercialized military message payloads carrying geospatial and unit organization data and the like can be triggered or provided a universal timing mechanism by applying the ubiquitous TCP/IP heartbeat. Once the TCP/IP heartbeat function is triggered by the intrinsic timer to get/put data, that data can be then collected for onward delivery by more current and flexible intelligent agents as found in newer P2P based protocols and transported over networks via the Simple Symmetric Transport Protocol (SSTP) thus enabling a universal homeland defense, homeland security alert, data and information exchange supporting method especially given the Department of Homeland Security"s recent purchase of twenty thousand seats of a P2P based product which includes intelligent agents or "bots"and runs on top of the TCP/IP stack.. Tools to configure the requisite unit or organizational structure and participation (Unit Task Orders), router management information base (MIB) and multicast groups (MCG) can be integrated or imbedded as tools into the selected enterprise software development/integration frameworks. While a particular product pur-

chased by the DHS (Groove Networks) is optimal, any XML messaging based P2P type product is a viable candidate. The necessary XML (SOAP) gateway to exchange XML payloads or (SOAP) messages between products is out of scope.

Brief Description of Drawings

[0005] Much of the functionality of the above drawing -- figure 1 -- has been generically explained in the background section and is intended to accompany the background section dialog. This diagram has less components and processes than it appears. This diagram is essentially what is briefed by the Army with annotations by the author relating the components as to their commercial equivalent descriptions. From left to right, MCS refers to the application that views the unit / organization location updates and generates the grouping of organizations (units) for missions (Unit Task Order / Reorder) hence the name Maneuver Control System. TIMS is the Tactical Internet Management System or the application that configures router management information bases (MIBS) and the associated multicast group entries. As stated in the patent application main body, alerts and changes in unit task orders to react to changing missions are routed via TCP multicast

groups. The INC or Internet Controller is a tactical router that can interface with radios with Global Positioning Sources. The C2R server is an LDAP server (Command and Control Registry in military speak). Finally the GTCS is the government message parser than generates the Variable Message Format messages. GTCS stands for Ground Tactical Communications Server. It is coupled with a message composition tool which can be substituted by a commercial forms engine. To summarize the functionality of this system in context with establishing a military heartbeat, an application chooses units from a hierarchical pick list. To distribute this unit organization and realizing that to reroute messages to units that affiliate with say adjacent organizations, routers MIB information needs reconfigured in routers which is accomplished by sending out VMF messages (K0.99 system configuration messages). The underlying TCP based mechanism provides the timing function, fields to get/set data from targeted hosts (FBCB2/TIMS platforms) and the transport mechanism as defined by router multicast groups. The LDAP (Lightweight Directory Access Protocol) server provides a more permanent storage mechanism, replication mechanism that the router MIB structure lacks. Note: the difference between

the military and commercial environments is that the military environment consists of proprietary messaging and network configuration tools other than that, TCP/IP is TCP/IP, APIs are APIs, methods and processes are etc, etc.

[0006] This diagram -- figure 2 -- shows the proposed tactical heartbeat mechanism in system using the same updated diagram from the previous patent application entitled "method to commercialize structured military messaging". The claimed functionality is again outside the dashed horizontal lines and shown inside a dash-dot lined square as to not suggest that the applicant is attempting to patent functionality that currently exists. Simply put, given the host environment will be running the ubiquitous TCP/IP stack, and given that a directory service / server is present to provide the LDAP/C2R functions, and given that the commercial realm configures multicast groups that are propagated by routers be they routers on the so called "tactical internet"or the internet, this patent application is suggesting and claiming that the same TCP/IP heartbeat mechanism be applied on the commercial side with the proviso that when the heartbeat"s ability to gather data from/send data is used, instead of routing the data to the Government Off the Shelf messaging process for dissemi-

nation across the system, that this TCP/IP and router function route the data as XML structures to the target host queue participating in multicast groups whereupon the P2P based system"s intelligent agents can act upon the data. The GOTS unique tools described in diagram one can be substituted with similar commercial tools interfaced or embedded into the enterprise software development/integration framework tool layer. As stated in the previous application, the VMF messages need converted by message gateways that change message types to XML schemas (for profiling and other purposes). Once the data is in XML schema form, the current commercial system will process this XML structure (message) by temporarily storing it in its underlying XML object store prior to onward distribution via the products XML (SOAP) relay sending only the changes given the intrinsic state management engine.

DETAILED DESCRIPTION

[0007] Expanding on this "heartbeat"function as employed by FBCB2 and the associated "Blue Force Tracking" (BFT), this functionality is made possible by an Application Program Interface (API) that is triggered by scripts that interact with an underlying mySQL database and a Global Positioning

Source (GPS) source/tactical radio. FBCB2 provides location updates correlated to unit task orders that govern how units organize for missions. FBCB2 is enabled by the underlying commercially ubiquitous TCP/IP heartbeat and is the principle means to gather data from and send data to identified host computers participating in IP multicast groups over the "lower tactical internet" read radio / satellite network. Since FBCB2 updates are distributed by way of the proprietary Government of the Shelf (GOTS) message parser over radio, wireless and satellite links on the "lower tactical internet) and passed to a Government developed suite of products called Information Dissemination Management (IDM) for dissemination over the "upper tactical internet" that is not likely to be widely fielded to or adopted by private industry collectively, these mechanisms are not suitable or flexible for widespread homeland security, commercial industry data exchanges. The patent application filed previous to this application, advocating a method to commercialize structured military messaging facilitates the use of the heartbeat mechanism to organize for and react to events that may threaten national security including targets in industry by providing the timing or trigger function a.k.a. the "heartbeat" that is

resident on every platform running TCP/IP. Given that the underlying heartbeat function is commercial and virtually universal, it can be applied not just to the low speed tactical radio and relatively low speed satellite links typical of FBCB2"s lower tactical internet environment but across the depth and breadth of the provinces of homeland defense and homeland security with the proviso that the military completes its conversion to XML schemas per the last patent application by this applicant.